CALEA and VoIP Outline

I. Introduction (Wiretapping, security)
II. National security
    CALEA background
        Explain the reasons for this regulation
        Why was it put in place?
        When?
        Who is obliged to comply?
    Patriot act (need more info)
        Explain the reasons for this regulation
        Why was it put in place?
        When?
        Who is obliged to comply?

III. Security enforcement in traditional networks
        PSTN

IV. VoIP and CALEA
        VoIP Introduction and Background
        VoIP and CALEA
        VoIP and PSTN
        Arguments for CALEA in VoIP
                VoIP and Patriot Act
        Arguments against CALEA in VoIP
        Cable, DSL and CALEA policy

V. Conclusions
        PSTN
        VOIP

Privacy Policy and the Public Switched Network

I. Introduction

Wiretapping the Public Switched Telephone Network (PSTN) has been a practice for many authorities around the world in fighting crime. In the United States, the value of this practice has ensured it a place in our policy, and modified the way carriers think when building their infrastructure. "Many governments, including the United States, require telephone companies to configure their networks so police can easily wiretap calls"(http://www.wired.com/news/politics/0,1283,31853,00.html). Proponents of wiretapping procedures argue for the benefits in fighting criminal activity in the courts, and are working to evolve the policy with the technology.

However, there are critics who claim this practice violates the rights of citizens, or provides an easy avenue for authorities to do so. Also, many feel that the current and/or expanded use of wiretapping by authorities will lead to a negative social change, built upon fear for the government. As the nation begins to face new challenges from changing threats and technologies, the line between protection and abuse gets finer. As such, regulators and activists continue to redefine what is protection, and what is abuse, of citizens and their rights.

National Security

Existing Privacy Protocol for the Public Switched Telephone Network allows the use of wiretapping by legal authorities, thanks to a court decision in *Katz v. United States.* "Prior to *Katz*, the Supreme Court had regarded wiretapping as outside the scope of the Fourth Amendment's restrictions on unreasonable searches and seizures (http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm)". After the *Katz* case, various acts and activities refined privacy protocol, defining who could perform electronic surveillance, how such surveillance should be carried out, and what responsibilities telecommunications carriers' had in providing assistance for surveillance.

Lawful surveillance is essential to effective law enforcement. Authorities must be authorized to access information from communications if such access will provide a measure of justice. Despite this authorization, authorities do not exercise such power on a regular basis, but only when the situation is most critical, or dire. "The federal government, District of Columbia, Virgin Islands, and forty-five states allow the use of

this technique, but only in the investigation of felony offenses, such as kidnapping, extortion, murder, illegal drug trafficking, organized crime, terrorism, and national security matters, and only when other investigative techniques, either can not provide the needed information or would be too dangerous" (http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm). Here one can see that although policy allows for wiretapping of suspects, enforcement agencies will try to avoid such intrusive methods on citizens if at all possible. However, they must be able to act if required.

CALEA

The Communications Assistance for Law Enforcement Act (CALEA), dealing entirely in defining carrier assistance, is a key bit of regulation in defining privacy policy for PSTN. The objective of CALEA implementation "…is to preserve Law Enforcement's ability to conduct lawfully-authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness"(http://www.askcalea.net/).

CALEA, for the first time, puts a large amount of responsibility on carriers to design and/or implement their assets in a way that will aid in surveillance. It also "…imposes certain responsibilities on the Attorney General of the United States, the Federal Communications Commission (FCC), telecommunications equipment manufacturers, and telecommunications support services providers" (http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm) to aid in authoritative surveillance. By doing this, one can see how policy is putting some responsibility on others to help it keep up with the dynamic world of telecommunications and technology. CALEA was an effective policy in that it provided some aid to enforcement agencies in gaining authorized access.

The advantages to Electronic surveillance of the PSTN are real, the evidence gained through such activity solid testament for prosecutors in a court of law. "In many instances, criminal activity has been either thwarted, or, if crimes have been committed, the criminals have been apprehended as a result of lawfully-authorized electronic surveillance"(http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm). Such surveillance provides unadulterated proof that one entity committed something illegal,

and therefore can be vital in the successful prosecution of any criminals. With defense attorneys attempting to establish reasonable doubt, the benefits of having a privacy policy on the PSTN that allows wiretapping works to establish a measure of certainty.

Many critics still site violations, or possible violations to the fourth amendment when speaking out against current policy to the PSTN. Wiretapping, it is claimed, allows searching an individual without a warrant or showing probable cause. To make matters worse, the suspect being searched is not even aware of this until after the work has been done. In one study done in 2002, it was found that out of more than 122,000 telephone conversations, almost 90 percent of which were determined to be non-incriminating, amounting to the unlawful search of many innocent citizens. "'It's useful to remember that the laws and limits we have in place were responses to the abuses of the past,' said Barry Steinhardt, Associate Director of the American Civil Liberties Union, arguing that more wiretapping will mean authorities will listen in on more innocent conversations"(http://archive.aclu.org/news/2002/w010802b.html).

In addition, the ACLU argues current policy for privacy may very well lead to dramatic effects upon the social structure of the country. "If people think that their conversations and their e-mails are their reading habits are being monitored, people will inevitably feel less comfortable saying what they think, especially if what they think is not what the government wants them to think" (http://www.aclu.org/Privacy/Privacy.cfm?ID=11054&c=130). While many may believe this view to be extreme, others see recent post-9/11 legislation as a precursor to this possible future.

Wiretapping techniques and the issues surrounding them continue to evolve as technology changes. In an effort to keep up with ever-mobile and tech-savvy criminals, individuals often set off a torrent of debate as they try to adapt policy. An article in 2002, illustrating officials attempting to expand wiretapping, lets one appreciate the troubles involved with ever-changing technology. "…former FBI agent George Vinson, says that many criminals now use cell phones to make just a few calls before switching to new phones to throw off investigators. Under current law, investigators would have to go back to a judge to seek new authority to begin monitoring the new

phones"(http://archive.aclu.org/news/2002/w010802b.html). Despite this argument, attempting to expand wiretapping brought critics and debate, hindering any change.

Regardless of the intrusion that some individuals may experience in their lives, the costs of avoiding these intrusions far outweigh the benefits. If we are to hold our protectors responsible for the welfare of our communities, then we must do our part in enabling such protectors with proper policy. The founding fathers, when drafting the fourth amendment, could not envision a time when enemies could communicate across the world while strolling down a main street, or would send in one individual to attack many innocent civilians. In addition, they knew this would be the case when they drafted their works, and specified a desire to see the documents they created grow with the nation. It is good to provide rights and freedoms to citizens, but the first part in doing that is protecting the people we wish to see free.

US Patriot Act

The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act was enacted in October 26, 2001, to further aid authorities in observing possible criminals. In contrast to CALEA, the Patriot Act is a broad, expansive bill that holds more than the traditional carriers accountable. Designed to broaden the surveillance capabilities of law enforcement following the terrorist attacks of September 11, 2001, the act designates any communications device used in connection to suspected terrorists as susceptible to investigation.

Additionally, institutions such as libraries must now aid authorities by disclosing patron activity, an action that contrasts sharply with their traditional practice. The fact that such diverse entities are now held responsible to enable authorities illustrates the broad powers the Patriot Act provides. Not only does it extend provisions provided by CALEA, it exports such provisions to a wide range of once-private mediums, both in and outside of the networked world.

The reasons for the Patriot Act are similar to that of CALEA, as both have been instituted to aid law enforcement with better technology and equipment. When working to pass the Act, Attorney General John Ashcroft cited it as necessary to provide better tools to authorities, saying "Technology has dramatically outpaced our statutes…Law enforcement tools created decades ago were crafted for rotary telephones--not e-mail, the

Internet, mobile communications and voice mail"(http://news.com.com/2100-1023_3-273778.html?tag=st_rn). Here, one can again see the constant struggle that takes place as we try to balance technology with policy, all the while trying to understand the impact that both can have upon civil rights.

An example of this delicate balance can be seen when examining the Patriot Act's attempt to broaden law enforcements ability to gather intelligence. Today, it is believed that policy must address the increased criminal communication through sophisticated technology, and so the Patriot Act attempts to address this need through various means, "…including "roving" wiretaps and the communications of computer trespassers"(http://news.com.com/2100-1023_3-273778.html?tag=st_rn).

Critics agree that this new policy makes it possible to agencies to abuse their rights by making unwarranted intrusions in communications, and incorrectly monitoring activity with single, broad court orders. This is because the Act creates "…new federal crimes, increase the penalties for existing federal crimes, and adjust existing federal criminal procedure, particularly with respect to acts of terrorism"(http://www.cdt.org/security/usapatriot/011210crs.pdf)

For example, while policy addresses the new threats from computer crime by categorizing it under terrorism, fear arises that legislation could be disproportionate to the computer crime, disregarding an individuals right to fair hearing and relative punishment. "Online vandals who deface a Web site could, conceivably, face a sentence of life imprisonment" (http://news.com.com/2100-1023_3-273778.html?tag=st_rn) because the Patriot Act offers punishments of up to life imprisonment for terrorism, with the statute of limitations removed.

The Patriot Act covers a wide range of other powers that authorities are now entrusted with, and is therefore accused of attempting to match policy to technology, with little to no regard toward civil rights. Currently, there is strong opposition on different fronts to the rights granted government agencies, and we may see the Patriot Act modified from it's current form in times to come.

Privacy Policy and Voice Over IP

VoIP Introduction and Background

Recently, FBI and other authorities have voiced concerns over communication traffic through new technology mediums. One major issue of concern is voice over IP. This new medium allows for communication to occur solely through the internet usually without ever passing through a single telephone switch. If left unmonitored, it could be a medium in which criminals and terrorists use to transmit information and communicate without any type of regulation. Because of new technologies such as VoIP, the issue of CALEA is brought up to ensure the safety of the public and to allow authorities to obtain needed information.

VoIP transmissions currently constitute about 10 percent of all the calls made in the US and about 2.5 millions subscribers (Trope). With these numbers, the VoIP arena will be definitely growing as the years progress. There have been debates and issues as to how to categorize VoIP. Some say that since it does not use the telephone network that telephone regulations should not apply and it should be considered an internet application. However, other proponents suggest that VoIP provide many of the same services that telephone systems do and regulations do need to applied in this new technology.

VoIP and CALEA

If implemented, CALEA would require companies that offer VoIP services to be compliant and have the necessary equipment that would allow authorities to wiretap the specified conversations. According to the AskCALEA website, CALEA is not about authority but about access. CALEA "seeks to ensure that after Law Enforcement obtains the appropriate legal authority, telecommunications carriers will have the necessary capability, and sufficient capacity, to assist Law Enforcement regardless of their specific systems or services (AskCALEA)."

VoIP and PSTN

VoIP has many ties to the standard public switched telephone network (PSTN). However, there are significant differences between the two that have to be addressed before CALEA and other regulations can be implemented. Currently CALEA is regulated only for telephone companies and still has yet to be decided for regulation on VoIP

(McCullagh, 2004). However, CALEA was written with the notion that new technologies will arise that will require regulation and monitoring. As mentioned previously, the two sides debate over whether VoIP should be categorized as solely an internet application where no telephone regulation should be applied or that it is considered an optional telephony method where regulations do apply.

VoIP uses the internet as the medium to make calls as opposed to PSTNs which use switches and wirelines. One way of making a phone call is to another VoIP user. They can be using a computer or a VoIP appliance phone. Through this method, the entire phone call is made over the internet. If the VoIP provider has the capabilities to interface with the PSTN, then a person with VoIP can call those with a regular phone as well.

Arguments for CALEA in VoIP

Most large VoIP providers have voluntarily complied with the FBI and other authorities to be within CALEA standards. However, a coalition of 12 smaller VoIP companies have told the FCC that with new industry changes coming ahead, they would need more time to be compliant with CALEA (McCullagh, 2004).

VoIP calls oftentimes do not cross into the PSTN and technically cannot be tapped (Charny). It is difficult to actually tap into a VoIP conversation because there is no actual line that is being used. The internet is the medium that is being used for VoIP and a number of different pathways can be taken in order to reach the destination. The phone calls are often encrypted and with the current technology is not feasible to be able to provide law enforcement with the content of the phone calls (Charny).

There are many issues the advocate the use of CALEA and wiretapping in VoIP. One of the major reasons and which also carries over from the PSTN side is to provide services that protect the country and aids law enforcement in gaining information critical for them to do their jobs. This is a general statement of why CALEA is in existence and why law enforcement is able to wiretap into our telephones now.

VoIP and Patriot Act

Another reason why CALEA will need to be implemented for VoIP is due to President Bush's Patriot Act (FBI). The Patriot Act was created after 9/11 which states that law enforcement can follow a person's communications through any phone as

opposed to tapping an individual's single phone number. This act significantly increases law enforcement's abilities to follow individual's phone and other communications wherever they go. Attorney General John Ashcroft stated that President Bush would veto any bill which would come into conflict with the Patriot Act (FBI). Thus, the Patriot Act extends the power of CALEA to anything that opposes it.

An issue brought up in Trope's article was concern about the interaction of regulation on exisiting PSTN and VoIP providers. "De-regulation of Internet services may allow baby bells to raise rates charged to ISPs for access to the copper wire that accesses subscribers' homes and businesses (Trope)." Thus, if Internet services and VoIP is not regulated, PSTN service providers may raise rates to level the playing field due to the charges and costs they have to incur from government regulation.

"They say that call content and caller identification could evade lawful electronic surveillance, and that VoIP jeopardizes the ability of federal, state, and local governments to protect public safety and national security against domestic and foreign threats," says Jonathan Adelstein a vocal FCC commissioner about VoIP (Poulsen).

Arguments Against CALEA in VoIP

Those that are against CALEA in VoIP have legimate claims as to why wiretapping and CALEA should not be implemented in VoIP networks. In general, the claim is that wiretapping and CALEA is intrusive and violates privacy issues when abused and used without reasonable justification. Oftentimes, with these abilities and technologies, they are often abused and used illegally. Privacy issues are an important issue concerning CALEA and VoIP. Information can be routinely collected for surveillance without any "investigatory predicate" (Trope). This allows for abuse among those that have this privilege. However, policies and strict enforcement will be able to maintain and regulate such monitoring.

One important issue that voices concern regarding CALEA and VoIP are data mining ties that go along with such wiretapping (FBI). Although not directly connected with VoIP, the ability to collect information and running analysis on such information can be done since VoIP is naturally connected to the internet and computers. With this natural connection, it is very easy to abuse this information which can lead to personal property or privacy violations.

Another important issue concerning CALEA and VoIP is that there is no guarantee that the data collected will be handled appropriately by VoIP providers or the FBI (Trope). Once the information is collected, handling, using and appropriate storage should be of concern to those that obtained such information. Officials that possess these abilities should maintain strict confidentiality and treat all information collected with the utmost care within the terms of appropriately doing their jobs. Neglect and abuse of collected information through CALEA is not an excuse for those with this privilege.

The "full pipe" issue is also a critical concern for those involved with CALEA and VoIP (Trope). Because VoIP and broadband cannot be isolated to a single line like PSTN, hundreds or thousands of people will be monitored and susceptible when specific data is collected and conversations are monitored. Currently the only feasible way to monitor VoIP conversations would be to tap into a large chunk of bandwidth which the desired VoIP conversation is a minute part of what law enforcement officials are targeting to be able to hear and monitor. This puts everyone at risk and brings about issues about whether or not this ability should be this legal and permissible.

Once regulated, VoIP is also subject to services and other systems that standard PSTN possess. Allowing wiretapping on VoIP networks will allow other statutes to take into effect such as taxation of the internet and mandating of 911 services, guaranteed access, remote area service, and service for the hearing impaired (Trope).

Cable, DSL and CALEA Policy

CALEA in other areas of telecommunications also have ties to VoIP. One such issue is that the court of appeals recently ruled that cable operators are telecommunications providers and subject to the same state and federal regulations (Trope). These cable operators provide telephone service through their systems and at first were not affected by the regulations normally enforced on standard PSTN such as CALEA. Now, cable operators may soon be required to be compliant with CALEA as well. Some companies such as Time Warner have begun to become compliant with CALEA(Charny, 2004). Also, there are current technologies like PacketCable which assist in wiretapping calls through cable (Ellis, 2003). In the case of DSL providers, telephone companies are usually those that maintain DSL lines so CALEA is not a new

idea for them. Requests to tap a DSL line have already been requested and made (Mccullagh and Charny, 2004).

Another interesting development in the broadband arena is the DCS1000 system, previously known as Carnivore. This system allows authorities to monitor customer's broadband usage and tap into their broadband service (McCullagh, 2003). With these developments in the broadband arena, there is only a matter of time before these regulations and technologies come down on VoIP.

Conclusions

Although there are legitimate claims against supporting CALEA in VoIP, these reasons are not enough to justify that the safety and welfare of others. Their safety should not be jeopardized through inhibiting law enforcement agencies to do their jobs. VoIP is a rapidly developing arena and still has a long way to go before being adopted widespread. Many different developments are being made and authorities are becoming more and more aware of these different technologies that need to be monitored to ensure national security (McCullagh and Charny, 2004). Most experts do agree that VoIP service will grow. With this kind of prediction, federal agencies and law enforcement have to implement some type of regulation that will ensure the safety of the public. Without such monitoring abilities, VoIP has the potential to be a rampant gateway for criminals to use and communicate without and repercussions. It also takes away an important information gathering tool from law enforcement if CALEA is not implemented in VoIP.

Works Cited

American Civil Liberties Union Newsbulletion. Retrieved February 29, 2004, from http://archive.aclu.org/news/2002/w010802b.html

AskCALEA. Retrieved February 28, 2004, from http://www.askcalea.com/index.html

Calea.org. Retrieved February 29, 2004, from http://www.calea.org/index.html

Charny, Ben. (2004 March 16). Cable taps into wiretap law. http://news.com.com/2100-1034-5173320.html

Charny, Ben (2004, February 13). VoIP: It's Not So Easy to Listen In. Retrieved February 28, 2004, from http://news.com.com/2100-7352-5159159.html

Doyle, Charles. (2001, December 10). Section by Section Analysis of the USA Patriot Act http://www.cdt.org/security/usapatriot/011210crs.pdf

Ellis, Lesile. (2003 April 21). CALEA and Cable: Part 2 http://www.translation-please.com/2003/0421_calea_II.html

FBI Urges FCC to Delay VoIP Proceeding Due to CALEA Concerns. Retrieved February 28, 2004, from http://www.alliancedatacom.com/news/fbi-urges-fcc-to-delay.asp

FCC Homepage. Retrieved February 29, 2004, from http://www.fcc.gov/calea/

Lemos, Robert. (2001, October 2). Revamped anti-terrorism Bill hits House http://news.com.com/2100-1023_3-273778.html?tag=st_rn

McCullagh, Declan (2003, July 29). FBI Targets Net Phoning. Retrieved February 28, 2004, from http://news.com.com/2100-1028_3-5056424.html?tag=mainstry

McCullagh, Declan (2004, January 8). Feds Seek Wiretap Access Via VoIP. Retrieved February 28, 2004, from http://news.com.com/2100-7352-5137344.html

McCullagh, Declan and Ben Charny. (2004 March 12). FBI adds to wiretap wish list. http://news.com.com/2100-1028-5172948.html

Poulsen, Kevin(2003, December 12). Will VoIP be Wiretap-ready? Retrieved February 28, 2004, from

http://www.securityfocus.com/news/7650

Trope, Konrad (2004, February). A New Chapter in the War on Terrorism: The FBI Wants Expanded Wiretapping Authority. Retrieved February 28, 2004, from http://practice.findlaw.com/tooltalk-0204.html

United States Department of Justice. Retrieved February 29, 2004, from http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm

United States Department of Justice. Retrieved February 29, 2004, from http://www.usdoj.gov/criminal/cybercrime/wiretap2510_2522.htm

University of North Carolina Course Page. Retrieved February 29, 2004, from http://www.unc.edu/courses/pre2000fall/law357c/cyberprojects/spring01/Carnivore/Legislative_History.htm

Wired Magazine Homepage. Retrieved February 29, 2004, from http://www.wired.com/news/politics/0,1283,31853,00.html